SECURE WEB GATEWAY (SWG)

Control and protect your users' web traffic.

To filter and protect

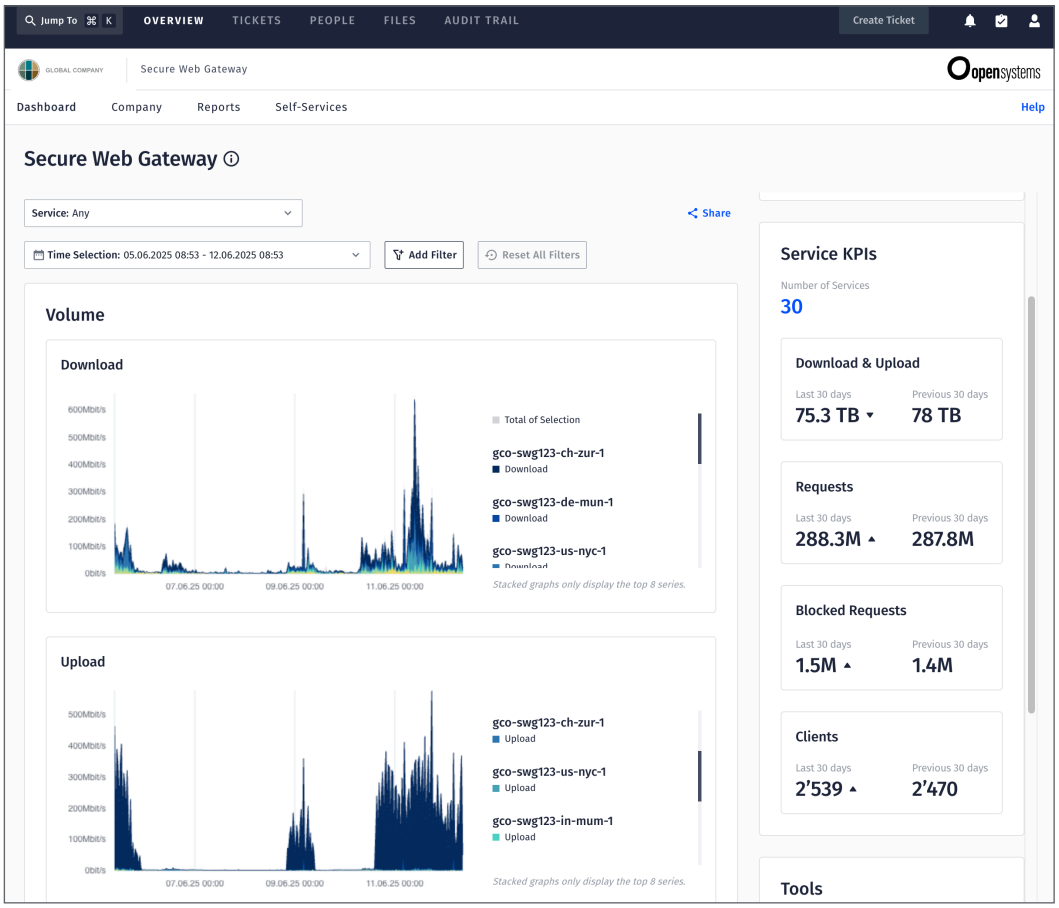
Protect your organization's network servers and end-user machines not just by filtering traffic from both the internal network and the internet – but by leveraging multiple security zones within the network itself.

The Secure Web Gateway acts as an intermediary enforcing an organization's internet access security policy for clients that request access to resources located on the public internet. Depending on the modules that are activated, it increases the level of protection of client machines against malicious content and restricts access to URL categories.

Core functions

This service provides a proxy server for HTTP and HTTPS traffic. TLS connections are decrypted, checked against the security policy, and forwarded through if granted. The company-wide distribution of the proxy configuration is supported with proxy auto-configuration (PAC). The PAC file is either delivered from the SWG appliance or through the SSE agent.

All the information for the on-prem and cloud Secure Web Gateway is in one place in the Mission Control Portal.



Secure Web Gateway dashboard.

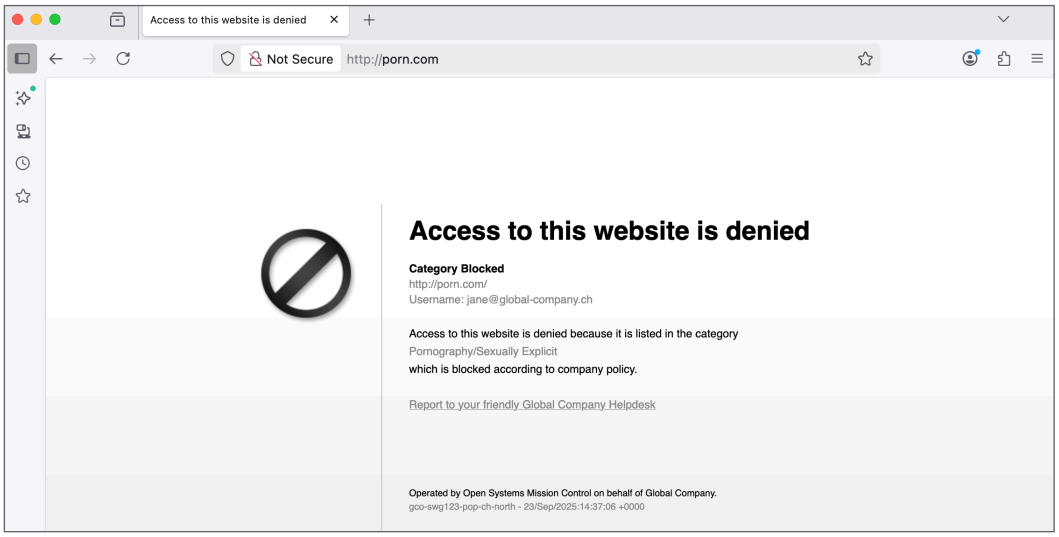
It shows how much traffic was downloaded and uploaded by an application, a domain, a city, or a client, with customizable filters. It is easy to share the customized dashboard via a URL or export its data to a CSV file.

Blocked entries based on IP addresses, domains, domain names or hostnames can be customized in the Secure Web Gateway. Additional flexibility and broader configuration options can be achieved with the URL Filter, introducing category-based access rules and customizable block lists and exclusion lists (that allow entries to bypass checks). Group and port access policies are granularly definable and assign access rules to groups of network resources such as IP addresses and ports.

SWG traffic metadata as well as platform metrics are constantly ingested by Open Systems' central data platform. The data is then processed and formatted to provide valuable insights.

The internet browsing policy can be visualized in the Mission Control Portal and distributed to all Secure Web Gateway enforcement points, independent of the deployment option (Cloud PoPs, VM appliance or on-premises appliance). This provides a unique global policy and, therefore, an efficient approach to global internet access policy enforcement.

If users go against policy or are faced with errors, the SWG displays error pages that inform users in a clear way about what happened, why, and what to do next. The error pages are configurable and, together with the report link, make it possible to set up an efficient support process that lowers operations effort.



Example of an error page that informs users about what happened, why and what to do next.

Monthly browser compliance and traffic volume reports provide an overview of the company's browser distribution and web traffic, and are tailored to an executive management audience. The figures are benchmarked against the overall performance of all Open Systems Secure Web Gateway services worldwide. The reports are downloadable in PDF and Excel formats, giving full portability and reusability to the statistical data.

Summary of SWG core functions	
HTTP and HTTPS proxy server	Full control over your HTTP and HTTPS traffic
HTTP and HTTPS protocol enforcement	Only compliant HTTP / HTTPS traffic is forwarded
Proxy Autoconfiguration (PAC) and Web Proxy Auto-Discovery Protocol (WPAD) support	Granular steering of web traffic depending on clients and servers
Application-aware policies	Easy implementation of SWG policies for applications like Microsoft 365, Salesforce, Zoom, etc.
Group-based policies	Enforcement of policies based on directory service group memberships or IP network segments

Summary of SWG core functions	
Customizable error pages	Corporate-branded error pages with clear troubleshooting information
IPv4 and IPv6 full support	Full support for IPv4, IPv6 and a mix of both
Port restriction	Granular control of TCP ports used for HTTP and HTTPS traffic

Threat Protection

By quickly detecting and blocking malicious entities, the risk of becoming infected is dramatically reduced. Open Systems curates several security feeds from well-known vendors, covering different attack vectors to conjointly secure the Open Systems DNS Filter, Secure Web Gateway and Email Security traffic.

Summary of Threat Protection[1]	
Standard Threat Protection	Set of feeds covering malware, phishing, potentially unwanted programs (PUPs) and spam
Advanced Threat Protection (Add-on)	Additional set of feeds covering 0-day attacks, newly released IOCs, fast-changing Command and Control (C&C) servers and short-living phishing websites

Platform

Open Systems Secure Web Gateway can be deployed in three ways: as a service through Open Systems Cloud PoPs, on customer premises through a hardware appliance, or in the customer's cloud environment through a VM. The SWG service offers great flexibility to accommodate web traffic anywhere and up to multi-gigabit speed. The Secure Web Gateway also offers dual-stack capability, which enables users to reach IPv6 sites on the internet from an IPv4 network.

User Authentication

Secure Web Gateway is available with the following protocols to authenticate users, and grant or disallow internet access:

1. **Single sign-on (SSO)**: for cloud PoP deployments
   Authentication via end-user agent through single sign-on (SSO) integrated identity provider (SAML, OpenID Connect (OIDC)).
2. **Microsoft-integrated (Kerberos)**: for VM and on-premises deployments
   Kerberos can seamlessly authenticate a supported client against the Secure Web Gateway by making use of an organization's Microsoft Entra ID infrastructure. The authentication takes place within the HTTP conversation with the help of the SPNEGO mechanism (HTTP Negotiate).
3. **Lightweight Directory Access Protocol (LDAP)**: for VM and on-premises deployments
   Remote Authentication Dial-In User Service (RADIUS). The LDAP authentication method uses the LDAP protocol. LDAP can authenticate a user against the Secure Web Gateway by making use of an organization's LDAP infrastructure. The user is presented with a pop-up window that requests the user credentials. Authentication is done by a bind operation to the LDAP directory. Internet policy memberships can be assigned to a user, based on LDAP group attributes.

1 Threat Protection is available for Email Security, SWG and DNS Filter.

Summary of User Authentication	
Single sign-on (SSO) for cloud PoP deployment	Authentication via end user agent through SSO-integrated identity provider (SAML, OIDC, LDAP, RADIUS)
Kerberos for on-premises and VM SWG deployment	Authentication via Microsoft's integrated authentication against Entra ID server
Basic authentication for on-premises and VM SWG deployment	Authentication via LDAP

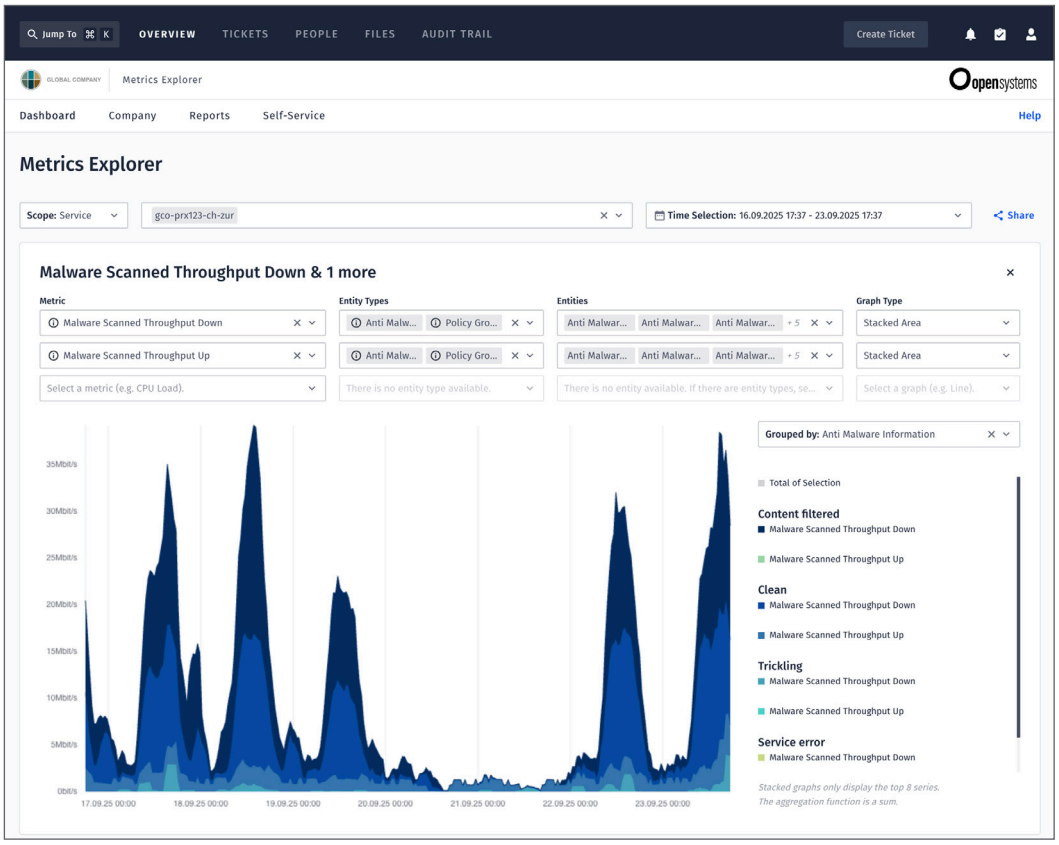
Policies

SWG configuration parameters are defined per group and will be enforced on every Open Systems Secure Web Gateway. This is used to distinguish malware protection, URL filtering and TLS Interception for different departments or groups of people. The group assignment is either based on the client IP address or the Entra ID / LDAP group.

Malware Protection

This feature performs malware protection with protocol scanning technologies for HTTP. It uses a combination of several filters to detect both known and unknown malware. Configuration options for specific characteristics of internet browsing traffic such as archive handling policies and media type filters can be defined and are visualized in the Mission Control Portal.

The customer portal features global and detailed statistics as well as drill-down capabilities to gauge the security posture and help mitigate threats.



Metrics Explorer showing malware scanning statistics for a Secure Web Gateway.

Summary of Malware Protection	
AI-enabled file scanning	Blocking of malware by using machine learning, heuristics and generics to identify malicious code, with near zero false positives
File archive protection	Filtering of special file archives (encrypted, nested, etc.)
Cloud Sandbox (Add-on)	Additional, advanced layer of web and email security, seamlessly integrated into standard file scanning of Secure Web Gateway and the Email Security service

Summary of Media Type Filter	
Web content policy	Blocking of content based on its type (e.g. executables, documents with active content, ...)

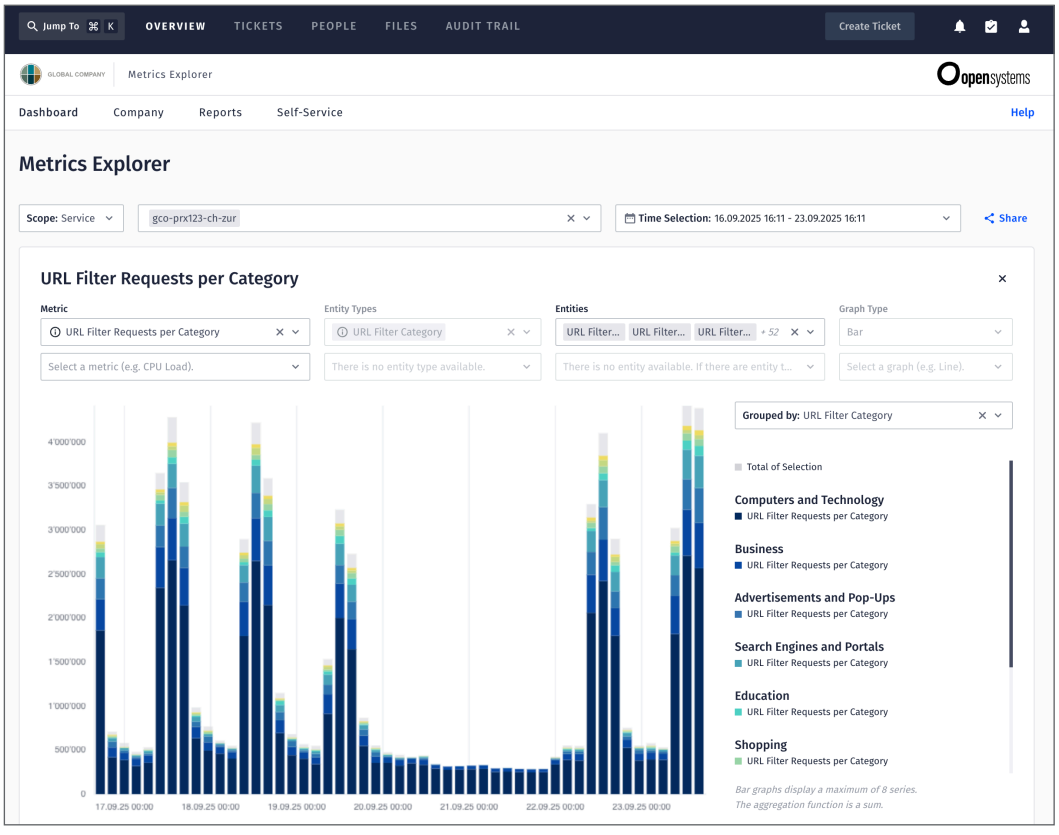
Cloud Sandbox

For more information, see the **Cloud Sandbox** datasheet.

URL Filter

The URL Filter enforces an organization's internet access policy and protects against risks associated with the employees' internet use. It reduces legal liability, enhances web security, increases productivity, and preserves bandwidth for business-related activities.

The URL Filter leverages categories that are curated by Open Systems to provide a comprehensive and proven source of millions of global URLs reducing the risk of unwanted access to certain websites.



Metrics Explorer showing URL Filter statistics for a Secure Web Gateway.

The Secure Web Gateway uses innovative cloud technology for a live update of its category database. Categories of previously unknown URLs are updated in near real time. New websites are automatically detected and forwarded to the vendor for categorization. A tool in the Mission Control Portal makes it possible to look up URL categories so that recategorizations can be requested.

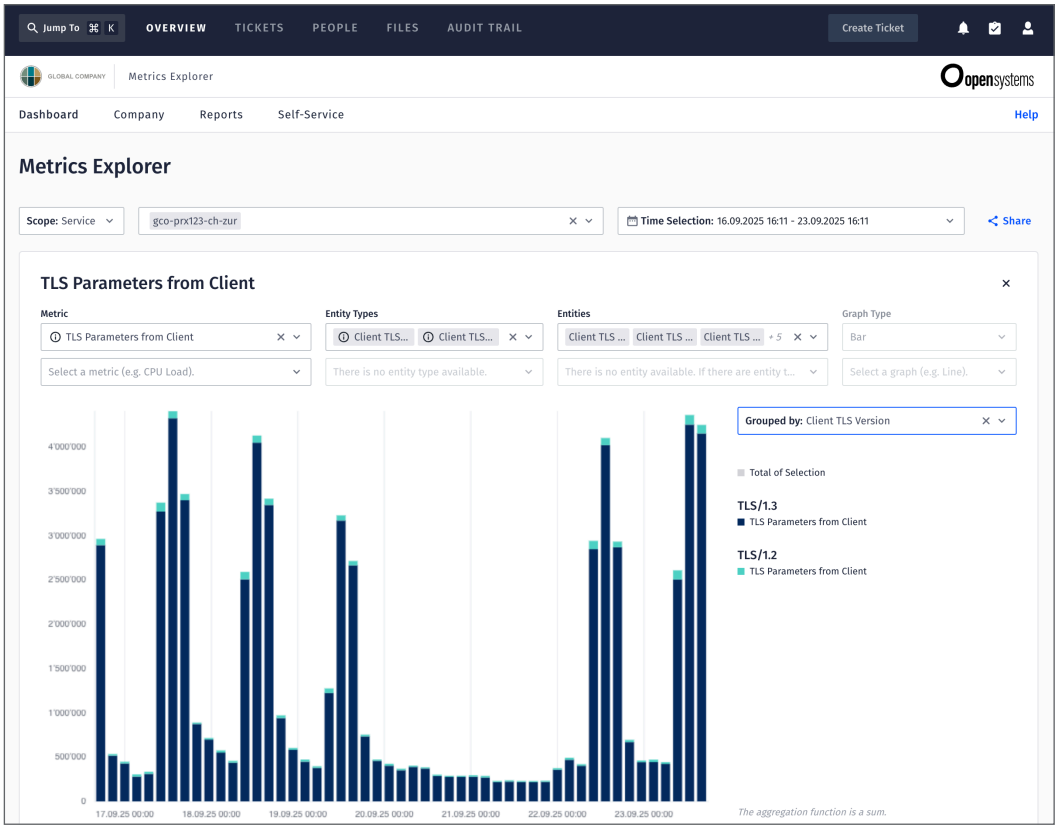
The monthly executive management report summarizes the total number of violation attempts and their top five categories. The number of connection requests and blocked attempts are shown for each category, giving a clear overview of the category statistics.

Summary of URL Filter	
Internet browsing policy	Blocking of content based on its category (e.g. Sports, Gambling, ...)
URL and domain policy	Blocking of specific URLs and domains

TLS Inspection

TLS Interception applies the existing security and internet usage policy to the HTTPS protocol and, therefore, enforces an organization's policy even for encrypted traffic.

TLS Interception makes it possible to validate server certificates and define customized actions to be taken for not fully trusted certificates. Depending on the policy, such certificates can be allowed, blocked, or the decision can be passed on to the user. SSL certificate mimicking uses the extensive built-in certificate handling in modern browsers. Instead of completely hiding a web server's SSL certificate from the user's visibility, certificate mimicking shows the user some critical information about the original server certificate, which helps the user decide whether to accept the server certificate.



Metrics Explorer showing TLS statistics for a Secure Web Gateway.

The Secure Web Gateway signs server certificates with its own certificate authority, which is set up during installation. The client machine is required to accept this certificate authority. Customer representatives manage the certificate authority acceptance processes.

All connections with client certificates need to be tunneled through without scanning.

Summary of TLS inspection	
Interception of TLS traffic	Decryption of HTTPS traffic for monitoring, scanning and enforcing policies on encrypted traffic
TLS policy	Enforcement of TLS protocol version and cipher
Certificate verification	Checks of server certificates, blocks of non-compliant access, and warning users about potentially suspicious websites

Web Traffic Tap (for on-premises and VM deployments only)

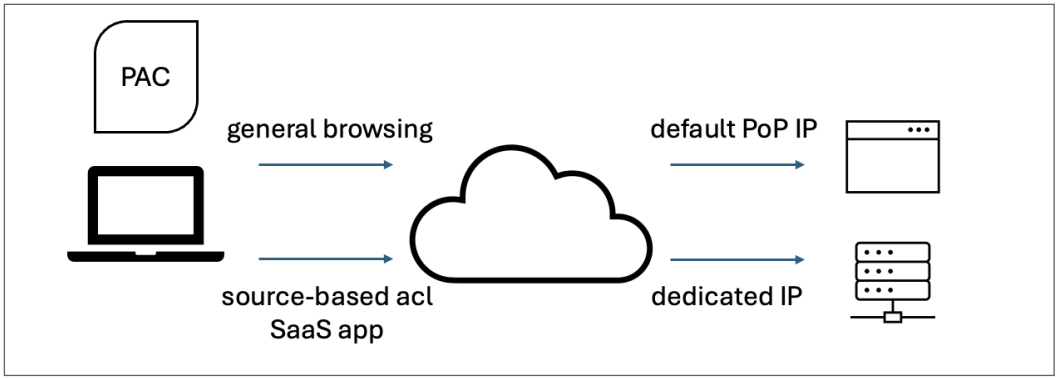
As the majority of web traffic is encrypted, network security monitoring solutions have limited visibility. In combination with TLS Interception, the Web Traffic Tap closes the blind spot and provides full visibility of all web gateway traffic including web traffic that is normally encrypted.

The Web Traffic Tap is a designated network interface on which simulated connections between the client and server can be passively monitored. The behavior is similar to what could be observed on the network if a client connected to a web server, with the difference that decrypted HTTPS traffic can be observed in plain text. Threat detection solutions are configured to monitor the web traffic on the Web Traffic Tap interface like they would be configured to monitor any other network traffic.

Dedicated IP for Cloud PoPs

Users connecting to the Secure Web Gateway via the Open Systems global Cloud PoPs are typically assigned an egress IP address from the local PoP. This IP is shared across multiple tenants, which works well for most browsing scenarios.

However, some organizations require source-based access control for specific applications, cloud services, or partner integrations. These scenarios depend on traffic originating from a customer-dedicated IP that can be allowlisted by external applications or third parties.



Dedicated IP feature enables customers to obtain exclusive IP addresses allocated per PoP.

The **Dedicated IP** feature enables customers to obtain exclusive IP addresses allocated per PoP. These IPs are:

- Managed by Open Systems
- Dedicated to the customer, never shared with other tenants or services
- Available in each PoP where the customer routes traffic

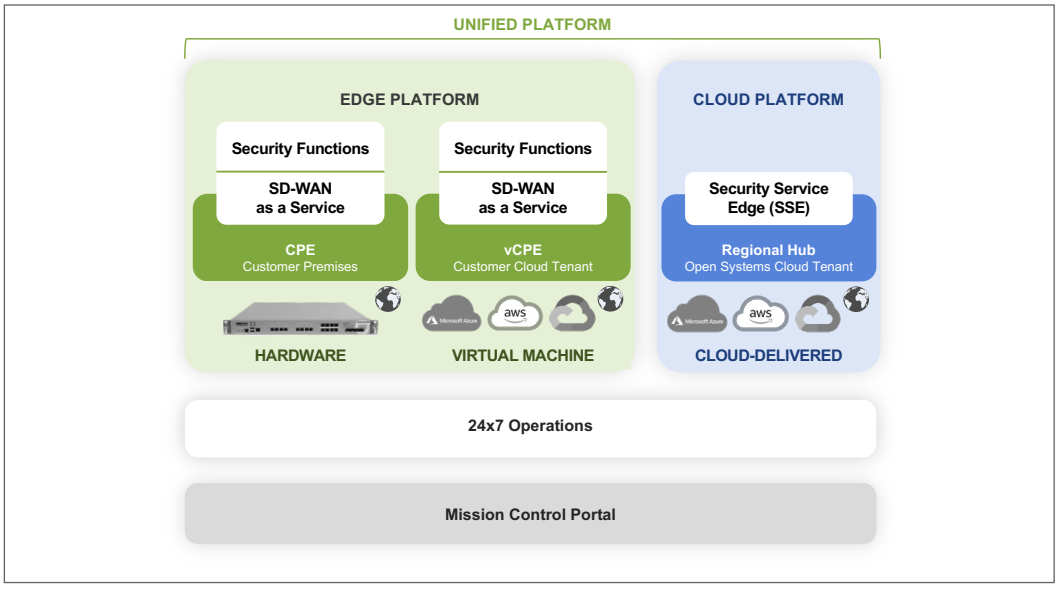
Customers can selectively route traffic to specific domains or applications through the dedicated IP, while allowing the rest of their traffic to continue using the default PoP IP. This allows fine-grained control over traffic paths based on business requirements.

To retain geo-awareness, it is recommended that general browsing and traffic that does not require source-based allowlisting continue to use the default PoP IP, which reflects the country the user is located in. When using a dedicated IP, however, the traffic will appear to originate from the PoP where the dedicated IP is allocated, regardless of the user's actual location.

Summary of Dedicated IP for Cloud PoPs	
Exclusive IP addresses allocated per PoP	For selective routing through a dedicated IP, depending on domains and applications.
Source-based access control	For specific applications, cloud services, or partner integrations so that a customer-dedicated IP can be allowlisted by external applications or third parties.

Service Management

For every service, Open Systems delivers flexible technology, maximum transparency, and around-the-clock network security and monitoring. It's an intrinsic part of a high-reliability organization.



Service Management is part of every Open Systems service.

Service Management closes the gap between security policy and operations, and reduces complexity. The service fee includes the following.

Platform

• **Edge Platform**	Services run on an Edge Platform whose location is flexible: • **Customer Premises Equipment (CPE)** Services run on premises or at a data center, on **extendable, industrial strength hardware for reliable 24x7 operations**. Mission Open Systems best practices ensure that a hardened operating system is deployed, where only essential tools and utilities are activated and, therefore, cannot lead to unexpected instability and compromised systems. The device is capable of booting different releases, which facilitates an effective fallback and rapid recovery if required. • **Virtual Customer Premises Equipment (vCPE)** Open Systems services can be provided **from the cloud**. Public clouds such as Microsoft Azure, Amazon Web Services and Google Cloud Platform are supported as well as private clouds. Mission Control makes sure that all appropriate security-related settings are up to date and configured correctly. The high availability option provides continuous connectivity if the Edge Platform fails.
• **Cloud Platform**	Fully managed, auto-scaling infrastructure with built-in security and zero-ops maintenance. Global, high-performance network ensure reliable, cost-effective service wherever your users are.

24x7 Operations

Highly skilled certified engineers in Mission Control monitor your systems proactively, ensure compliance with your security policy and work according to clearly defined processes in order to review and perform global changes that are driven by the dynamic needs of your organization.

After extensive testing procedures, all required security updates and patches are installed on a regular basis, always keeping the systems and services up to date. All environment-specific configurations are automatically generated, based on the configuration database operated by Mission Control. This is an essential part of an efficient disaster recovery process because it makes it possible to generate and reinstall an identical configuration in a very short time.

Installation

- Definition of technical configuration
- Definition of the administrative contacts and escalation procedures
- Creation of the network topology diagram
- Preconfiguration, delivery and functional verification tests of the Open Systems service with all required hardware and software components

24x7 monitoring

- 24x7 proactive monitoring, event notifications (by email or SMS), automatic log file analysis and reporting
- Prompt response to detected critical events
- Unlimited number of escalations, tickets, support calls
- Direct support by Mission Control Engineers

Change management

- Enforced change management processes by comprehensive ticketing system and built-in sign-off procedures
- Review of change requests by Mission Control Engineers, clarifications and feedback in case of hidden risks
- Strong user authentication with audit trail

Troubleshooting and maintenance

- Real-time auditability with integrated ticketing system
- Debugging of incidents within the periods defined in the SLA
- Replacement of defective or outdated hardware and restoring of functionality
- Analysis, testing and installation of software patches and upgrades
- Predefined disaster recovery processes

Reporting and logging

- Real-time executive overview with geographic distribution
- Real-time network utilization and system load statistics
- Real-time reporting of configuration settings and logs
- Compliance report: Service Organization Controls 1 Type 2 (SOC 1 Type 2)

Coverage of technology risk

- Hardware and software are replaced free of charge if defective, outdated or if the quality or availability of the implemented systems are no longer guaranteed by the manufacturer

Mission Control Portal

The state-of-the-art web portal makes it easy to communicate with Mission Control. The portal provides transparency over your network and applications in real time, including reports and tools that support the implementation and management of global IT security and availability.

Summary of Mission Control Portal features	
Service overview	Detailed service overview of SWG statistics and KPIs
Configuration overview	Comprehensive overview of SWG settings and parameters
Logs Explorer	View details of every web request globally
URL Tracker	Runs a simulated HTTP / HTTPS request for any given URL to check policy and connection results
URL category lookup and recategorization	Look up a category for any given URL with possibility to request a recategorization if needed
Self-service policy changes	Direct editing of block lists and exclusion lists

For more information, see the **Service Management** fact sheet.

Edge Platform Capacities

Each IP address is counted as a user. A typical proxy traffic mixture is assumed, where 100 users add up to 5 Mbit/s and 25 requests/s (daily maximum of the per-hour average). These numbers can vary with different usage patterns, and more powerful hardware might be required.

Dedicated platform
Deployment option: M

- Recommended for up to 800 users

Shared platform
Deployment option: L

- Recommended for up to 2,500 users

Deployment option: S

- Recommended for up to 300 users

Deployment option: XS

- Recommended for up to 50 users

Platform Node: XXS

- Recommended for up to 5 users

Cloud Pops
See "**Fair use policy**" under Cloud Pop Connection Agent.

Overview of deployment options	
Cloud PoPs	Service delivered from Open Systems global SWG PoPs
Virtual Machine	Service delivered from customer cloud tenant in Microsoft Azure, Amazon Web Services or Google Cloud Platform
On premises	Service delivered from customer premises in rack appliance for data centers or large offices, or silent appliance suitable for small offices
Unified monitoring and seamless experience	Independent of the deployment options, SWG can be globally monitored and controlled under one portal. Users also experience the same level of service everywhere

Cloud PoP regions

- **US**: East US, South Central US, Central US, West US
- **Europe**: Germany West Central, Switzerland North, UK West, France Central
- Southeast Asia
- Australia
- Brazil South
- South Africa North

Cloud PoP Connection Agent

Open Systems SSE Agent automatically connects users to their closest point of presence. Available for Mac OS, Windows, and Linux (Ubuntu).

Fair use policy	
On premises and VM deployments	A typical service configuration and traffic mixture is assumed. These numbers can vary with different usage patterns or feature configurations and more powerful hardware/VMs might be required.
Cloud PoPs	The usage per subscribed user is expected to be less than 200% of the usage of an average user (i.e. 6 GB per user per month). If the usage exceeds this acceptable amount, available options need to be discussed.

Open Systems is certified for ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018.

HIPAA Compliance Verified by VanRein Compliance 2025

Approved for public use.

Open Systems reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Note: Due to the licensing and export restrictions of our technology suppliers, we are not permitted to provide services in certain sanctioned countries. The specific countries affected depend on each supplier's compliance requirements. We therefore refer to the respective suppliers' license terms, which may also apply to end users.